ABSTRACT

Methods and apparati are provided for use in determining "Squared Weil pairings" and/or "Squared Tate Pairing" based on an elliptic curve, for example, and which are then used to support cryptographic processing of selected information. Significant improvements are provided in computing efficiency over the conventional implementation of the Weil and Tate pairings. The resulting Squared Weil and/or Tate pairings can be substituted for conventional Weil or Tate pairings in a variety of applications.